NORTH-HOLLAND

Eigenvectors of Circulant Matrices of Prime Dimension*

Andrew J. Lazarus†

2745 Elmwood Avenue
Berkeley, California 94705

Submitted by Richard A. Brualdi

ABSTRACT

In this note we show that the eigenvectors of circulant matrices of prime dimension can be expressed succinctly in the notation of classical cyclotomy.

Matrices $A = (a_{i,j})$ where $a_{i,j} = a_{0,j-i}$ are called *circulant matrices.* (Matrix indices will start at 0 and always be taken modulo the size of the matrix.) Each row is the right rotation of the row above. To save space, we will write

$$A = cir(a_0, a_1, a_2, \ldots, a_{n-1})$$

if A is the $n \times n$ circulant matrix whose first row is $(a_0, a_1, \ldots, a_{n-1})$. Then $n \times n$ circulants form a ring. Three special circulants are the identity matrix I, the all-ones matrix $J = cir(1, 1, \ldots, 1)$, and the rotate-right operator $Z = cir(0, 1, 0, \ldots, 0)$.

Fix $\zeta_n = exp(2\pi i/n), i = \sqrt{-1}$. The $\mathbb{Q}[\zeta_n]$-eigensystem of a circulant matrix is well known. Define column vectors $\boldsymbol{\zeta}^{(j)}$ by

$$\boldsymbol{\zeta}^{(j)} = \left(1, \zeta_n^j, \zeta_n^{2j}, \ldots, \zeta_n^{(n-1)j}\right), \qquad j = 0, 1, \ldots, n-1.$$

*Partially supported by the Employment Development Department, State of California.

†E-mail:lazarus@nli.com.

655 Avenue of the Americas, New York, NY 10010
0024-3795/95/$9.50
SSDI 0024-3795(93)00234-Q

THEOREM 0 (Spottiswood, 1853). *If $A = cir(\mathbf{a})$ is an $n \times n$ circulant matrix, a complete system of (right) eigenvectors for A over $\mathbb{Q}[\zeta_n]$ is given by $\boldsymbol{\zeta}^{(j)}, j = 0, \ldots, n-1$. The eigenvector $\boldsymbol{\zeta}^{(j)}$ corresponds to the eigenvalue $\mathbf{a} \cdot \boldsymbol{\zeta}^{(j)}$.*

Proof. See, e.g., Davis [2, Theorem 3.2.2]. ∎

Theorem 0 as it stands is not, however, entirely satisfactory. The eigenvalues of a circulant matrix may lie in a proper subfield of $\mathbb{Q}[\zeta_n]$.

Denote the smallest field containing the eigenvalues by K, and let $e = [k:\mathbb{Q}]$. We will find a complete system of eigenvectors in K^n when n is a prime p.

We review the notation of cyclotomy. Given a factorization of $p = ef+1$, the *cyclotomic classes C_ν of degree e* are defined by

$$C_\nu = \{g^{ek+\nu} \bmod p : k = 0, \ldots, f-1\}, \qquad \nu = 0, \ldots, e-1,$$

where g is any primitive root *mod* p. We write $ind\, h = \nu$ if and only if $h \in C_\nu$. The *Gaussian periods* η_ν are defined by

$$\eta_\nu = \sum_{h \in C_\nu} \zeta^h, \qquad \nu = 0, \ldots, e-1.$$

Set

$$\mathbf{v} = (p-1, -1, -1, \ldots, -1) \in \mathbb{Q}^p$$

and

$$\boldsymbol{\eta}^{(\nu)} = (f, \eta_\nu, \eta_{\nu+ind\,2}, \ldots, \eta_{\nu+ind(p-1)}) \in K^p.$$

THEOREM 1. *An eigensystem in K is given by*

	Eigenvalue	*Multiplicity*	*Eigenvectors*
$K = \mathbb{Q}$	$\mathbf{a}_0 + (p-1)\mathbf{a}_1$	1	$\zeta^{(0)}$
	$\mathbf{a}_0 - \mathbf{a}_1$	$p-1$	$Z^k\mathbf{v}, 0 \le k \le p-2$
$K = \mathbb{Q}[\alpha] \neq \mathbb{Q}$	$\sum_{j=0}^{p-1} \mathbf{a}_j$	1	$\zeta^{(0)}$
	$\alpha^{(\nu)}, 0 \le \nu \le e-1$	f *each*	$Z^k\boldsymbol{\eta}^{(\nu)}, 0 \le k \le f-1$

where α is an irrational eigenvalue of A, and $\alpha^{(\nu)}$ runs through its Galois conjugates. Furthermore, $K = \mathbb{Q}$ if and only if there exist r and s such that $A = rI + s(J - I)$.

Proof. Suppose that A has only rational eigenvalues. Since $\zeta, \zeta^2, \ldots,$

ζ^{p-1} is a basis for $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$, $\mathbf{a}\cdot\boldsymbol{\zeta}^{(1)} \in \mathbb{Q}$ implies that $\mathbf{a}_1 = \mathbf{a}_2 = \cdots = \mathbf{a}_{p-1}$ while $\mathbf{a}_0$ is free. Setting $r = \mathbf{a}_0$ and $s = \mathbf{a}_1$, we have $A = rI + s(J - I)$.

Let A be any matrix of the form $rI + s(J - I)$. From Theorem 0 the eigenvalues are just the $\mathbf{a} \cdot \boldsymbol{\zeta}^{(j)}$, and this equals $r + (p-1)s$ if $j = 0$ and $r - s$ otherwise. By closure $\mathbf{v} = \sum_{j=1}^{p-1} \boldsymbol{\zeta}^{(j)}$ is an eigenvector, as is

$$Z^k\mathbf{v} = \sum_{j=1}^{p-1} Z^k\boldsymbol{\zeta}^{(j)} = \sum_{j=1}^{p-1} \zeta^{jk}\boldsymbol{\zeta}^{(j)}, \qquad k = 1, \ldots, p-2.$$

It remains to show that

$$\{Z^k\mathbf{v} : k = 0, \ldots, p-2\}$$

is a linearly independent set. The transformation matrix from the $\boldsymbol{\zeta}^{(j)}$, $j = 1, \ldots, p-1$, to the $Z^k\mathbf{v}$, $k = 0, \ldots, p-2$, is given by

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \zeta^1 & \zeta^2 & \cdots & \zeta^{p-1} \\ \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \vdots & \vdots & & \vdots \\ \zeta^{p-2} & \zeta^{2(p-2)} & \cdots & \zeta^{(p-1)(p-2)} \end{bmatrix},$$

which is an invertible Vandermonde matrix.

Now suppose $K \neq \mathbb{Q}$. The rational eigenvalue is obtained from $A\boldsymbol{\zeta}^{(0)} = (\sum_{j=0}^{p-1} \mathbf{a}_j)\boldsymbol{\zeta}^{(0)}$. The minimal polynomial of α divides the minimal polynomial of A, so the Galois conjugates of α are also eigenvalues. We will show in the following lemmas that the eigenspace of α, as well as its conjugates, is generated by $Z^k\boldsymbol{\eta}^{(\nu)}$ for some ν and $k = 0, \ldots, f-1$. Since this has dimension f, and eigenvectors belonging to distinct eigenvalues are independent, $\boldsymbol{\zeta}^{(0)}$ and the $Z^k\boldsymbol{\eta}^{(\nu)}$ are a full system of eigenvectors in K^p. [The rational case which we have already done is essentially identical; the eigenvector $\mathbf{v}$ is merely the specific value of all $\boldsymbol{\eta}^{(\nu)}$ when $f = p - 1$, and the eigenvalue $\mathbf{a}_0 + (p-1)\mathbf{a}_1$ coincides with $\sum_{j=0}^{p-1} \mathbf{a}_j$.] ■

LEMMA 1. *The principal cyclotomic class C_0 is the subgroup of $\mathbb{Z}/p\mathbb{Z}^*$ of index e, and the other classes are its cosets.*

Proof. Immediate from the definition. ■

Since K is abelian, it contains α and all of its conjugates. For $1 \leq h \leq p-1$, write σ_h for the automorphism of $\mathbb{Q}[\zeta]$ defined by $\sigma_h : \zeta \mapsto \zeta^h$.

LEMMA 2. *For $h \in C_0, \sigma_h$ fixes K.*

Proof. Immediate from the previous lemma and Galois theory. ∎

LEMMA 3. *If $\zeta^{(h)}$ is an eigenvector corresponding to α, so is $\zeta^{(h')}$ for all $h' \in C_{ind\, h}$.*

Proof. The automorphism $\sigma_{h^{-1}h'}$ maps $\zeta^{(h)}$ to $\zeta^{(h')}$. By Lemma 1, if h and h' are in the same class, $h^{-1}h' \in C_0$. Hence, by Lemma 2, $\sigma_{h^{-1}h'}$ fixes $\alpha \in K$. Now apply $\sigma_{h^{-1}h'}$ to the equation $A\zeta^{(h)} = \alpha\zeta^{(h)}$. ∎

LEMMA 4. $\displaystyle\sum_{h \in C_\nu} \zeta^{hj} = \eta_{\nu + ind\, j}$.

Proof.

$$\sum_{h \in C_\nu} \zeta^{hj} = \sum_{k=0}^{f-1} \zeta^{jg^{ek+\nu}} = \sum_{k=0}^{f-1} \zeta^{g^{te+ind\, j} g^{ek+\nu}} \qquad \text{for some } t,$$

and the lemma follows. ∎

LEMMA 5. *With $\zeta^{(h)}$ as in Lemma 3, $Z^k \eta^{(ind\, h)}, k = 0, \ldots, f-1$, are linearly independent K-eigenvectors belonging to α.*

Proof. From the previous lemma,

$$\eta^{(ind\, h)} = \sum_{h' \in C_{ind\, h}} \zeta^{(h')},$$

and from Lemma 3 and closure, this is an eigenvector of α. Since $Z^k \zeta^{(h)} = \zeta^{hk} \zeta^{(h)}$, we have from Lemma 4 that

$$\begin{aligned} Z^k \eta^{(ind\, h)} &= Z^k \sum_{h' \in C_{ind\, h}} \zeta^{(h')} \\ &= \sum_{h' \in C_{ind\, h}} \zeta^{h'k} \zeta^{(h')}, \end{aligned}$$

which is also an eigenvector of α by closure.

Let $\{h_1, h_2, \ldots, h_f\}$ be an enumeration of $C_{ind\, h}$. The transformation matrix from the $\zeta^{(h_\mu)}$, $\mu = 1, \ldots, f$, to the $Z^k \eta^{(ind\, h)}, k = 0, \ldots, f-1$, is

given by

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \zeta^{h_1} & \zeta^{h_2} & \cdots & \zeta^{h_f} \\ \zeta^{2h_1} & \zeta^{2h_2} & \cdots & \zeta^{2h_f} \\ \vdots & \vdots & & \vdots \\ \zeta^{(f-1)h_1} & \zeta^{(f-1)h_2} & \cdots & \zeta^{(f-1)h_f} \end{bmatrix},$$

which is an invertible Vandermonde matrix. ■

This concludes the proof of Theorem 1. ■

COROLLARY. *The minimal polynomial of A either splits into linear factors or is a linear factor times one irreducible factor.*

REMARK. Theorem 1 settles the eigenvector questions posed by D. H. Lehmer in [3], as well as eigenvectors of the additional circulants he introduced in [4, 5]. (It is easy to match up the eigenvalues found by Lehmer with our eigenvectors.) A paper of Carlitz [1] contains other examples of prime-dimension circulants.

Lehmer [3] defined *matrix paraphrases* $H^{(\nu,e)}$ of the Gaussian periods as follows: Define the vector $\mathbf{h}^{(\nu,e)}$ by the rule

$$\mathbf{h}_j^{(\nu,e)} = \begin{cases} 1 & j \in C_{\nu,e}, \\ 0 & \textit{otherwise}, \end{cases} \qquad j = 0, \ldots, p-1, \quad \nu = 0, \ldots, e-1,$$

and set $H^{(\nu,e)} = cir(\mathbf{h}^{(\nu,e)})$. Using these matrix paraphrases, we prove an analogue of Gauss's result that the periods η_ν are a basis for K over $\mathbb{Q}$.

THEOREM 2. *The ring of $p \times p$ circulant matrices whose eigenvalues have degree (over $\mathbb{Q}$) dividing e is additively generated by I and the $H^{(\nu,e)}$.*

Proof. Suppose $A = cir(\mathbf{a}) = rI + \sum_{\nu=0}^{e-1} s_\nu H^{(\nu,e)}$. Since $\mathbf{h}^{(\nu,e)} \cdot \boldsymbol{\zeta}^{(1)} = \eta_\nu$ (where η_ν is a Gaussian period of degree e), Theorem 1 implies that the eigenvalues of $\mathrm{H}^{(\nu,e)}$ are the η's of degree e. It follows that an eigenvalue of A may be written as

$$\alpha = r + \sum_{\nu=0}^{e-1} S_\nu \eta_{k_\nu},$$

where it is possible but irrelevant to determine which period η_{k_ν} is. Obviously $\alpha \in K$.

To prove the converse, we use the fact that the η's of degree e are a $\mathbb{Q}$-basis of K when $[K:\mathbb{Q}] = e$. Hence $\mathbf{a} \cdot \boldsymbol{\zeta}^{(1)} = \sum_{j=0}^{p-1} \mathbf{a}_j \zeta^j$ is in K if and only if $\mathbf{a}_j = \mathbf{a}_{j'}$ whenever $j' \in C_{ind\, j}$. Setting $r = \mathbf{a}_0$ and $s_\nu = \mathbf{a}_{g^\nu}$, we have the desired decomposition of A. ■

The case of eigenvalues that are all rational can be subsumed in this theorem by defining $H^{(0,1)} = J - I$.

REFERENCES

1 L. Carlitz, Some cyclotomic matrices, *Acta Arith.* 5:293–308 (1959).
2 Philip J. Davis, Circulant matrices, Wiley, New York, 1979.
3 D. H. Lehmer, A matrix paraphrase of cyclotomy, *Acta Arith.* 53:357–366 (1990).
4 ———, A matrix paraphrase of Kloosterman sums, *Acta Arith.* 56:83–92 (1990).
5 ———, Matrix paraphrases, *Linear and Multilinear Algebra* 28:251–264 (1991).

Received 27 January 1993; final manuscript accepted 26 August 1993